Browser Extensions

Browser extensions are small packages of software that interact with web browsers like Google Chrome, Mozilla Firefox, MacOS Safari, etc. They add functionality to your browser, allowing you to customize your browsing experience.

Why use them?

Some well-vetted and trusted browser extensions can drastically improve the security and privacy of your web activity. Installing and configuring these extensions can help:

- Protect your passwords
- Encrypt your browsing
- Reduce tracking
- Block advertisements
- Alert you to a site's known privacy practices

How they work

The source code of browser extensions works with the source code of a browser in order to amend certain default browsing activities. The technical mechanisms behind this depend on the function of the extension. For instance, an ad blocker extension might compare the code of a webpage against known ad patterns, and block the chunks of code that are known to be ads. By contrast, the HTTPS Everywhere plugin searches for a given URL, determines if an encrypted version of that URL is available, and if so redirects the unencrypted URL to the encrypted URL. Information on how browser extensions work is generally readily available where they are downloaded, especially if the extensions are open-source.

How to use them

Browser extensions should be downloaded and installed in the browser's web store. These are trusted repositories for the software

- For Firefox: https://mzl.la/3138OIV
- For Chrome: http://bit.ly/2IHaod3
- For Safari: https://apple.co/2nE4MJx (redirects to App Store)

Extensions are not currently officially supported by browser developers for mobile devices.

Disclaimers

Although browser extensions should go through peer review before being made available, there is a chance that some may be malicious. As when downloading anything, be sure that the product is well-reviewed, recommended, and from a credible source.

You can also improve the privacy and security of your browsing by using a trusted browser (e.g., Firefox) and configuring its settings. For instance, you can set your browser to "Do not track" and use a different search engine such as DuckDuckGo that doesn't associate your browsing history with an identifiable persona.

Examples (Search for these in your browser’s extension manager)

- Privacy Badger – Blocks ads, cookies, and invisible trackers
- Cookie AutoDelete – Deletes cookies from a browser session when you close the tab
- HTTPS Everywhere – Reroutes all requests to secure URLs if they exist
- DuckDuckGo Privacy Essentials – Provies tools for privacy along with a grading system for web sites based on their privacy practices
- AdNauseum – Obfuscates browsing data by simulating anonymous clicks on every ad blocked by…
- UBlockOrigin **–** Helps you manage ad blocking, trackers, and cookies

Related resources

- HowStuffWorks’ guide to surfing the web anonymously: http://bit.ly/33h9xYu.
- Mozilla’s guide to browser extensions: https://mzl.la/2M71GXN.
- NNDEV’s Internet Browser Privacy Tips: http://bit.ly/2OBYsNx.
- University of Michigan’s guide to securing your browser: http://bit.ly/2nBl31F.